



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/590,415

10/20/2006

Nicolas Popp

026970-003210US

7016

94224

7590

04/13/2010

TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

NIGH, JAMES D

ART UNIT

PAPER NUMBER

3685

MAIL DATE

DELIVERY MODE

04/13/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

1. This communication is in response to amendments and remarks filed on 16 February 2010.

Claim Status

2. Claims 1, 2 and 6 have been amended. Claims 10 and 11 have been added. Claims 1-11 are currently pending and are presented for examination on the merits.

Response to Arguments

3. Applicant's argument with regard to the 35 U.S.C. § 101 rejection of claims 1-9 has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

4. Applicant's argument with regard to the 35 U.S.C. § 103 (a) rejection of claims 1-9 has been fully considered but is not persuasive.

Prior to addressing Applicant's argument, Examiner is producing a definition of the word "token" from the Microsoft Computer dictionary:

token n. 1. A unique structured data object or message that circulates continuously among the nodes of a token ring and describes the current state of the network. Before any node can send a message, it must first wait to control the token. See also token bus network, token passing, token ring network. 2. Any nonreducible textual element in data that is being parsed—for example, the use in a program of a variable name, a reserved word, or an operator. Storing tokens as short codes shortens program files and speeds execution.

As such nothing within Applicant's claims excludes a software "token". The language in fact is simply a recitation of non-functional descriptive material as the recitation regarding how the one-time passwords are generated is not part of the

Art Unit: 3685

claimed method steps. As such it is not entitled to patentable weight, and therefore cannot be used to distinguish the claimed invention from the prior art.

With regard to claim interpretation, per MPEP § 2173.02 regarding "clarity and precision": "Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire"; in addition per MPEP § 2173.04 "breadth is not indefiniteness".

Also with regard to the interpretation of words of a claim will be given their "plain meaning" unless such meaning is inconsistent with the specification (MPEP § 2111.01) "Although claims of issued patents are interpreted in light of the specification, prosecution history, prior art and other claims, this is not the mode of claim interpretation to be applied during examination. During examination, the claims must be interpreted as broadly as their terms reasonably allow. *In re American Academy of Science Tech Center*, 367 F.3d 1359, 1369, 70 USPQ2d 1827, 1834 (Fed. Cir. 2004).

Applicant's disclosure regarding the word token (page 1, line 30 "A token is a device that can be used to authenticate a user"; page 2, lines 22-26 "An embodiment of the present invention includes a protocol for generating One Time Passwords ("OTPs") at a hardware device that can be used to authenticate a user. The OTPs are generated by a token, 'which can be a physical device' that includes mechanisms to prevent the unauthorized modification or disclosure of the software and information that it contains, and to help ensure its proper functioning.) only recites what a token could be, but recites no explicit definition of what it is. Furthermore the original claims as recited did not incorporate into the claims limiting language that would have placed the traditional

Art Unit: 3685

Microsoft Computer Dictionary definition of a token outside the broadest reasonable interpretation.

As claims 1 and 6 are directed towards a method and not an apparatus, if arguably the token were to be interpreted as structure the recitation of structure (in this case Applicant's "token") must manipulatively affect the method in order to receive patentable weight "As to the rejection of the claims on the prior art references, we do not agree with the appellant that such structural limitations as are not disclosed by the references should be given patentable weight. This argument is applicable to claims drawn to structure and not claims drawn to a method. To be entitled to such weight in method claims, the recited structural limitations therein must affect the method in a manipulative sense and not to amount to the mere claiming of a use of a particular structure, which, in our opinion, is the case here", *Ex parte Pfeiffer*, 135 USPQ 31 (BdPatApp&Int 1961). Such is not the case with claims 1 and 6, particularly in light of the fact per Applicant's disclosure the only relevant teaching regarding the structure is that a token "can be a physical device". Moreover Examiner does not agree that with Applicant "a ticket is not similar to a token" as per the Microsoft computer dictionary a token is a data structure. Thus Examiner sees Applicant's remarks as providing evidence that the Applicant within the originally presented claims did not, as required by 35 U.S.C. § 112, 2nd paragraph, "set forth the subject matter that applicants regard as their invention" (See MPEP § 2171, also MPEP § 2172 II "Evidence that shows that a claim does not correspond in scope with that which applicant regards as applicant's invention may be found, for example, in contentions or admissions contained in briefs or

Art Unit: 3685

remarks filed by applicant, *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 55 USPQ2d 1279 (Fed. Cir. 2000); *In re Prater*, 415 F.2d 1393, 162 USPQ 541 (CCPA 1969).

Moreover as the recitation of claim 1 “where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password” is simply non-functional descriptive material as it merely describes the secret and count without reciting method steps; again the recitation is not entitled to patentable weight. See MPEP § 2106 II C and 2111.04.

As the cited Matyas reference discloses “workstations” (4:24-36) that generate the count and shared secret value to form the concatenated value (5:17-25), the Matyas reference meets Applicant's definition of a “token” as a workstation is a physical device. Newcombe in paragraphs 0058 and 0064-0066 teaches that the shared ticket is shared between a server and a client device (again physical devices). Therefore even in light of Applicant's remarks the combination of Matyas and Newcombe teaches claim 1.

5. Applicant's argument with regard to claim 2 regarding the recitation “if the calculated...” has been fully considered but is not persuasive. The recitation is directed to optional language which is not limiting “Language that suggests or makes optional

Art Unit: 3685

but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation”, MPEP § 2106 II C.

6. Applicant's argument with regard to claim 2 regarding a token based upon a serial number or user name has been fully considered but is not persuasive. Applicant's argument is only directed at the Matyas reference when a combination of Newcombe was provided. In response to applicant's arguments against the Matyas reference individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

7. Applicant's argument that the next action should be made non-final has been fully considered but is not persuasive. Applicant, as evidenced by remarks, failed in the originally presented claims to set forth the subject matter as required by 35 U.S.C. § 112, 2nd paragraph; in addition the Applicant is placing reliance on recitations not entitled to patentable weight and optional language. Moreover Applicant has attacked reference individually instead of in combination. Examiner also maintains that the cited combination of Matyas and Newcombe teach invention as claimed. Therefore this action will be made final.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 3685

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al. (U.S. Patent 5,953,420, hereinafter referred to as Matyas) in view of Newcombe (U.S. Patent PG Publication 2003/0172269, now U.S. Patent 7,392,390, hereinafter referred to as Newcombe).**

10. As per claim 1

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses the count number that increases monotonically (Figure 4, 5:17-25)

Matyas explicitly discloses the count number that increases monotonically with the number of One Time Passwords generated and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password (Figure 4, 5:17-25)

Matyas explicitly discloses hashing and truncating the result (5:26-31, 5:60-64)

Matyas discloses a token (4:24-36)

Matyas does not explicitly disclose where the secret is uniquely assigned to token and is shared between the token and an authentication server.

Newcombe teaches where the secret is uniquely assigned to token and is shared between the token and an authentication server. (0051, 0058, 0064-0066, 0068, 0072, 0091)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

“where the secret is uniquely assigned to a token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the number of One Time Passwords generated by the token and increases monotonically at the authentication server with each calculation by the authentication server of a One Time Password” is simply non-functional descriptive material “Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability

[T]he critical question is whether there exists any new and unobvious functional relationship between the printed matter and the substrate” *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry*, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II

11. As per claim 2

Matyas explicitly discloses receiving a request for authentication (2:35-57, 5:1-10, 5:46-59, 7:25-37)

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses calculating the one time password based on count values and the secret (Figure 4, 5:17-25)

Matyas explicitly discloses a token (4:24-46)

Matyas explicitly discloses incrementing the count (5:46-59)

Matyas explicitly discloses retrieving a count (5:46-59)

Matyas explicitly discloses retrieving a secret (6:62-65)

Matyas explicitly discloses calculating a one-time password based upon retrieved values of the count and the secret corresponding to the token (4:24-46, 5:17-30, 5:46-59)

Matyas explicitly discloses comparing the calculated one time password with the received one time password (6:45-61)

Matyas explicitly discloses that if the calculated and received password match that the request is authenticated (6:45-61).

Matyas, while disclosing authentication, does not explicitly disclose an authentication server or serial numbers

Newcombe teaches a serial number uniquely associated with a token (IP address, 0025, 0048, 0051)

Newcombe teaches a personal identification number associated with a user (password, 0057-58, 0065-0067)

Newcombe teaches an authentication server (0047, 0057)

Newcombe teaches where the secret is retrieved by the authentication server based upon the serial number (0025, 0040-0041)

Art Unit: 3685

Matyas while disclosing a count does not explicitly disclose recalculating, Newcombe does not explicitly teach incrementing the count and recalculating; however Newcombe teaches a window of acceptable values for time with which recalculation can occur and authenticate the client (0059, 0068, 0070, 0097). Thus a predictable result (*KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007)) of Matyas and Newcombe would be to substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable for the purpose of enabling improved authentication in a distributed environment.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

However the recitations beginning with the word "if" are merely reciting optional language these are not-limiting and are not entitled to patentable weight MPEP § 2106 II C.

12. As per claims 3 and 7

Newcombe teaches an SHA-1 hash function (0029-0030, 0068, 0103)

13. As per claims 4 and 8

Newcombe teaches a symmetric key (0028, 0032).

14. As per claims 5 and 9

Art Unit: 3685

Newcombe teaches “an acceptable time window” which would encompass a predetermined number of times for authentication (0059, 0068, 0070, 0097).

15. As per claim 6

Matyas explicitly discloses receiving a request for authentication (2:35-57, 5:1-10, 5:46-59, 7:25-37)

Matyas explicitly discloses concatenating a secret with a count (Abstract, 2:29-49, 5:17-31, 5:39-59)

Matyas explicitly discloses calculating the one time password based on count values and the secret (Figure 4, 5:17-25)

Matyas explicitly discloses retrieving a count based on a username (certificate and public value) (4:47-67, 5:46-59, 6:22-65)

Matyas explicitly discloses retrieving a secret based on a user name (6:22-65)

Matyas explicitly discloses comparing the calculated one time password with the received one time password (6:45-61)

Matyas explicitly discloses that if the calculated and received password match that the request is authenticated (6:45-61).

Matyas, while disclosing authentication and users does not explicitly disclose personal identification numbers. Newcombe teaches a personal identification number associated with a user (password, 0057-58, 0065-0067)

Matyas while disclosing a count does not explicitly disclose recalculating, whereas Newcombe does not explicitly teach incrementing the count and recalculating; However Newcombe teaches a window of acceptable values for time with which

Art Unit: 3685

recalculation can occur and authenticate the client (0059, 0068, 0070, 0097). Thus a predictable result (*KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007)) of Matyas and Newcombe would be to substitute the count value for the time value, perform the incrementing of the count and recalculate to determine if the count was acceptable for the purpose of enabling improved authentication in a distributed environment.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method for establishing an authenticated shared secret value between a pair of users of Matyas with the method for binding Kerberos style authenticators to single clients of Newcombe for the purpose of enabling improved authentication in a distributed environment.

However as the recitations beginning with the word "if" are merely reciting optional language these are not-limiting and are not entitled to patentable weight MPEP § 2106 II C.

16. As per claims 10 and 11 Matyas discloses wherein the secret is uniquely assigned to the token (4:24-36, 5:17-25, 46-59); however this recitation is simply non-functional descriptive material.

Please note:

A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Applicant(s) are reminded that optional or conditional elements do not narrow the claims because they can always be omitted. See *e.g.* MPEP §2106 II C: “Language that suggest or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. [Emphasis in original.]”; and *In re Johnston*, 435 F.3d 1381, 77 USPQ2d 1788, 1790 (Fed. Cir. 2006) (“As a matter of linguistic precision, optional elements do not narrow the claim because they can always be omitted.”).

Pertinent Art Not Cited

17. Ginter et al. (U.S. Patent 5,892,900) teaches portable electronic appliances (254:5-255:5, 255:60-256:11, 256:32-38)

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 3685

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D. NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on Monday-Friday 6:30 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt II can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAMES D NIGH/
Examiner, Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685